UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/628,729	07/28/2003	Anne Kirsten Eisentraeger	MS1-1280US	4013

22801 7590 01/12/2007

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	01/12/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 01/12/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)	
	10/628,729	EISENTRAEGER ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-63* is/are rejected.

7)☒ Claim(s) *4, 8, and 12* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see att*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Pursuant to USC 131, claims 1-63 are presented for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 3/22/2004 is being considered by the examiner.

Specification

3. The disclosure is objected to because of the following informalities: there is a typographic error in the abstract on line 2, "using the result so support" should read --using the result to support--. Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-63 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding independent claims 1, 5, and 9, the claimed invention as a whole must accomplish a practical application and must produce a useful, concrete, and tangible result. In this instance, the claimed invention merely recites a step of determining and a step of

"cryptographically processing selected information based on said determined..." cryptographically processing seems to be directed to an abstract idea that is not tied to a technological art, environment, or machine which would result in a practical application producing a useful, concrete, and tangible result. For instance, applicant's specification page 7, lines 14-17 indicates cryptographic processing for implementing the invention such as key generation; the mere fact of generating key is not tied to a tangible result by itself. Applicant's specification page 6, lines 20-22 indicates figure 3 as illustrating an exemplary process for use in a curve based cryptosystem for implementing the invention. Figure 3 as described on page 15, line 21 et seq. is pertaining to cryptographic algorithm, the algorithm pre se is not a statutory subject matter unless is tied to a technological art, environment, or machine which would result in a practical application producing a useful, concrete, and tangible result. See MPEP § 2106. Claim 9, although directed to an apparatus, the claim limitations seem to be directed to an abstract idea without limitation to a practical application as explained above because the claim merely recites calculating and at least partially support cryptographically processing stored information.

Regarding independent claims 13, 30, and 47, the claimed invention as a whole must accomplish a practical application and must produce a useful, concrete, and tangible result. In this instance, the claimed invention merely recites steps of determining which are directed to an abstract idea that is not tied to a technological art, environment, or machine which would result in a practical application producing a useful, concrete, and tangible result. See MPEP § 2106.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-7, and 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Non-Patent Literature to Gerhard Frey, Michael Muller, and Hans-Georg Ruck; "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems" IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 45, NO. 5, JULY 1999; Pages 1717-1719 (hereinafter **Frey et al**).

As per claim 1, Frey et al substantially teaches a method comprising: *determining at least one Squared Tate pairing for at least one hyperelliptic curve* (see page 1719, left column first two paragraphs) showing computation of Tate pairing for a hyperelliptic curve as mentioned on (see page 1718, left column, last paragraph prior to part II). **Frey et al** discloses using the Tate Pairing for computation of discrete logarithm which can be interpreted as a cryptographic process (see page 1718, right column, Remark 2.4 first paragraph) and further

discloses that the improved Tate Pairing can be used to reduce the discrete logarithm problem for elliptic curves (see page 1719, right column, paragraph 1). **Frey et al** suggests using the Tate pairing in cryptographic applications in which the Weil Pairing does not work (see page 1718, left column, part II, Remark 2.2) as explained in more details by Menezes et al in "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", also (Applicant's IDS). **Frey et al** does not explicitly state *cryptographically processing selected information based on Tate Pairing*. Elliptic curves have been known to be used in Public Key Cryptography as disclosed in Menezes' publication. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the improved Tate Pairing of **Frey et al** for cryptographically processing selected information. One of ordinary skill in the art would have recognized the advantages as disclosed by Frey et al above to implement Tate Pairing for finding groups of points on an elliptic curve to construct public key cryptosystems as known in the art (see also Menezes' Publication).

As per claim 2, Frey et al discloses computing Tate Pairing for a hyperelliptic curve over a field F (see pages 1717-1718, part I) that meets the recitation of *wherein said Squared Tate pairing is defined for at least one hyperelliptic curve C of genus g over a field K* (see page 1718, left column, last paragraph prior to part II), a hyperelliptic curve by definition has a genus g.

As per claim 3, Frey et al discloses *wherein determining said Squared Tate pairing further includes: forming a mathematical chain for m, wherein m is a positive integer and an m-*

*torsion element D is fixed on Jacobian of said hyperelliptic curve C (*see pages 1717-1718, part I). (Page 1718, right column, last paragraph shows $m=p^k$ which meets the recitation of a mathematical chain as interpreted by Examiner).

As per claims 5-7, claims 5-7 recite the same limitations as claims 1-3 respectively except for implementing the claimed method in a computer-implementable program. **Frey et al** discloses (page 1719, part III first paragraph) using a computer to implement the Tate Pairing. Therefore claims 5-7 are rejected on the same rationale as the rejection of claims 1-3.

As per claim 9, Frey et al substantially teaches an apparatus (computer) comprising memory configured to store information suitable for use with using a cryptographic process; logic operatively coupled to said memory and configured to calculate at least one Squared Tate pairing (see page 1719, part III first paragraph) for at least one hyperelliptic curve (see page 1719, left column first two paragraphs) showing computation of Tate pairing for a hyperelliptic curve as mentioned on (see page 1718, left column, last paragraph prior to part II). **Frey et al** discloses using the Tate Pairing for computation of discrete logarithm, which can be interpreted as partially support cryptographic processing (see page 1718, right column, Remark 2.4 first paragraph) and further discloses that the improved Tate Pairing can be used to reduce the discrete logarithm problem for elliptic curves (see page 1719, right column, paragraph 1). **Frey et al** suggests using the Tate pairing in cryptographic applications in which the Weil Pairing does not work (see page 1718, left column, part II, Remark 2.2) as explained in more details by Menezes et al in "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", also

(Applicant's IDS). **Frey et al** does not explicitly state cryptographically processing selected information based on Tate Pairing. Elliptic curves have been known to be used in Public Key Cryptography as disclosed in Menezes' publication. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the improved Tate Pairing of **Frey et al** for cryptographically processing selected information. One of ordinary skill in the art would have recognized the advantages as disclosed by Frey et al above to implement Tate Pairing for finding groups of points on an elliptic curve to construct public key cryptosystems as known in the art (see also Menezes' Publication).

As per claim 10, Frey et al discloses computing Tate Pairing for a hyperelliptic curve over a field F (see pages 1717-1718, part I) that meets the recitation of *wherein said Squared Tate pairing is defined for at least one hyperelliptic curve C of genus g over a field K* (see page 1718, left column, last paragraph prior to part II), a hyperelliptic curve by definition has a genus g.

As per claim 11, Frey et al discloses *wherein determining said Squared Tate pairing further includes: forming a mathematical chain for m, wherein m is a positive integer and an m-torsion element D is fixed on Jacobian of said hyperelliptic curve C (*see pages 1717-1718, part I). (Page 1718, right column, last paragraph shows $m=p^k$ which meets the recitation of a mathematical chain as interpreted by Examiner).

Allowable Subject Matter

6. **Claims 4, 8, and 12** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims, and if rewritten to overcome the rejection(s) under 35 U.S.C. 101, set forth in this Office action. Claims 4, 8, and 12 in the application are deemed to a nonobvious improvement of implementing Tate Pairing on the Jacobian of hyperelliptic curve. The claims comprise a mathematical chain form m and an m-torsion element D "*wherein said mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain*" so as to provide a significant speed-up over contemporary implementation of the Tate Pairing for hyperelliptic curve; and therefore, contain allowable subject matter.

6.1 **Claims 13-63** would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 101, set forth in this Office action. Independent claims 13, 30, and 47 in the application are deemed to a nonobvious improvement of evaluating Tate Pairing on the Jacobian of hyperelliptic curve. The claims comprise "*determining a Jacobian J(C) of said hyperelliptic curve C, and wherein each element D of J(C) contains a representative of the form A-g(P_0), where A is an effective divisor of degree g; and determining a plurality of functions $h_{j,D}$ that are iterative building blocks for the formation of a function $h_{m,D}$ in order to evaluate v_m which is a Squared Tate pairing*" so as to provide a significant speed-up over contemporary implementation of the Tate Pairing for hyperelliptic curve; and therefore, contain allowable subject matter.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-Form 892).

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carl Colin
Patent Examiner
January 5, 2007